

## University of Groningen

### Just integrating or integrating justice?

Seepma, Aline

DOI:  
[10.33612/diss.128074337](https://doi.org/10.33612/diss.128074337)

**IMPORTANT NOTE:** You are advised to consult the publisher's version (publisher's PDF) if you wish to cite from it. Please check the document version below.

*Document Version*  
Publisher's PDF, also known as Version of record

*Publication date:*  
2020

[Link to publication in University of Groningen/UMCG research database](#)

*Citation for published version (APA):*

Seepma, A. (2020). *Just integrating or integrating justice? Understanding integration mechanisms in criminal justice supply chains*. [Thesis fully internal (DIV), University of Groningen]. University of Groningen, SOM research school. <https://doi.org/10.33612/diss.128074337>

#### Copyright

Other than for strictly personal use, it is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), unless the work is under an open content license (like Creative Commons).

The publication may also be distributed here under the terms of Article 25fa of the Dutch Copyright Act, indicated by the "Taverne" license. More information can be found on the University of Groningen website: <https://www.rug.nl/library/open-access/self-archiving-pure/taverne-amendment>.

#### Take-down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Downloaded from the University of Groningen/UMCG research database (Pure): <http://www.rug.nl/research/portal>. For technical reasons the number of authors shown on this cover page is limited to 10 maximum.

# 3

## DESIGNING DIGITAL PUBLIC SERVICE SUPPLY CHAINS: FOUR COUNTRY-BASED CASES IN CRIMINAL JUSTICE<sup>1</sup>

<sup>1</sup> This chapter is published as:

Seepma, A.P., de Blok, C., & van Donk, D.P. (2020). Designing digital public service supply chains: four country-based cases in criminal justice. *Supply Chain Management an International Journal*, forthcoming.

## ABSTRACT

*Many countries aim to improve public services by use of information and communication technology (ICT) in public service supply chains. However, the literature does not address how inter-organizational ICT is used in redesigning these particular supply chains. The present chapter explores this important and under-investigated area. An explorative multiple-case study was performed based on 36 interviews, 39 documents, extensive field visits and observations providing data on digital transformation in four European criminal justice supply chains. Two different design approaches to digital transformation were found, which are labelled digitization and digitalization. These approaches are characterized by differences in public service strategies, performance aims, and how specific public characteristics and procedures are dealt with. Despite featuring different roles for ICT, both types show viable digital transformation of public service supply chains. Additionally, the application of inter-organizational ICT is found not to automatically result in changes in the coordination and management of the chain, in contrast to common assumptions. This study is one of the first to adopt an inter-organizational perspective on the use of ICT in public service supply chains. The findings have scientific and managerial value because fine-grained insights are provided into how public service supply chains can use ICT in an inter-organizational setting. The study shows the dilemmas faced by and possible options for public organizations when designing digital service delivery.*

### 3.1 | Introduction

Successfully implementing information and communication technology (ICT) in time, within budget and as intended has proven to be difficult in public service supply chains. Despite huge governmental investment in ICT, there is little evidence that the many years of spending on ICT infrastructure have led to long-term gains in either efficiency or effectiveness (Karwan & Markland, 2006; Venkatesh *et al.*, 2012). This is a major cause of concern because public supply chains, such as tax, healthcare, and criminal justice, are supposed to spend public money effectively and carefully. Until now, research on the use of ICT in public services has mainly focused on single organizations or on digitizing citizen-government linkages, e.g., using e-mail in internal and external communications, moving from paper-based to electronic record-keeping, or implementing electronic self-service systems (Dunleavy *et al.*, 2006; Lindgren & Jansson, 2013; Lupo & Velicogna, 2018). Accordingly, research largely ignores inter-organizational linkages and services. Following Zhang *et al.* (2011, p. 1217), ICT is defined as “a family of technologies used to process, store and disseminate information, facilitating the performance of information-related human activities, provided by, and serving both the public at-large as well as the institutional and business sectors (Salomon & Cohen, 1999)”. The redesign of paper-based processes and inter-organizational information flows into their ICT supported and enabled equivalents is defined as ‘digital transformation’ (Janowski, 2015; Vial, 2019). This frequently involves redesign of business operations and supply chain processes and affects (inter-)organizational structures (Matt *et al.*, 2015). The present chapter examines the under-investigated area of digital transformation in public service supply chains.

The subject of public service supply chains and their digital transformation is at the cross-roads of several related streams of research, i.e., public management, service operations management, service supply chain management, and information management. Despite their relevance to the understanding of public service supply chains and digital transformation, each of these research streams ignores important aspects related to this subject, as discussed below. First, characteristics of public services studied in public management are important because public service delivery is bounded by legal structures, political and regulated processes and procedures, and predetermined roles and responsibilities of organizations (Boyne, 2002; Dawes, 2009; Gil-Garcia & Sayogo, 2016; Yang & Maxwell, 2011). However, to date, this field lacks empirical investigation of inter-organizational public service delivery processes (Osborne *et al.*, 2012; Osborne *et al.*, 2016). Second, service operations management focuses mainly on service delivery by single organizations, ignoring the inter-organizational perspective relevant to many public services (Machuca *et al.*, 2007). Although the inter-organizational perspective is present in service supply chain management literature, (Baltacioglu *et al.*, 2007; Ellram *et al.*, 2004; Giannakis, 2011), that literature stream emphasizes links with customers (Grönroos & Voima, 2013; Maull *et al.*, 1993; Sampson & Spring, 2012; Voss *et al.*, 2008; Wang *et al.*, 2015) and gives limited attention to public settings (Fu *et al.*, 2013). Finally, compared to physical supply chains, for which ICT

and inter-organizational ICT have been acknowledged as critical for streamlining and managing the supply chain (Gunasekaran & Ngai, 2004; Zhang *et al.*, 2011, 2016), supply chain management literature has paid less attention to supply chains providing services. So far, this limited research has addressed the digital redesign and use of ICT within public organizations (Karwan & Markland, 2006), the relationship to customer-citizens (Ponsignon *et al.* 2018; Venkatesh *et al.*, 2012), and normative maturity models (Iannacci *et al.*, 2019). Thus, despite the potential benefits for public service settings, the inter-organizational nature of many public services is mostly ignored, and digital transformation in inter-organizational public services (hereafter: public service supply chains) has not been well-investigated. Therefore, more research regarding the potential and role of ICT systems in public service supply chains is needed (Karwan & Markland, 2006).

Consequently, the main aim of the present study is to answer the question: How do public service supply chains redesign their joint service delivery processes into digital processes? As indicated, ICT and digital transformation are defined widely. In the context of public service supply chains, the focus is on the use of electronic tools and communications that enable change from a paper-based flow of information towards a digital-based flow of information. This study's focus is on the use of ICT enabling digital information flows between public service organizations, including automated access and communication between digital databases and information systems. Generally, a transformation process of this kind is characterized by a gradual rather than disruptive change process and entails a transition from 'not digital' to 'as digital as possible'.

The starting point for the present study is the approach taken by Karwan and Markland (2006). They find that information technology applied in conjunction with a unified set of service operations concepts (i.e., service strategy, service delivery system characteristics, and performance measures) enables simultaneous improvements in efficiency and maintenance of equity in public services. Here, this perspective is extended to joint service delivery to acknowledge that public service delivery is increasingly a process involving several organizations (Osborne *et al.*, 2012; Voets *et al.*, 2008) that act as a supply chain (Callender, 2011; De Blok *et al.*, 2015). Further, this study combines insights from the aforementioned literature streams, i.e., public management, information management, service operations management, and service supply chain management. Empirically, the study relies on an extensive, explorative multiple-case study based on 36 interviews, 39 documents, several field visits, and observations across four European criminal justice supply chains that were digitally transforming their processes. The criminal justice supply chain provides an excellent example of a public service in which different organizations have to work together. Criminal justice organizations deliver their services based on intensive inter-organizational flows of information that are comparable to, for example, the delivery of social services or taxation. Another reason criminal justice is an interesting case is that many governments have aimed to move criminal justice processes in the direction of digital service delivery (e.g. European Commission, 2019).

The present study makes several important contributions to the understanding of service supply chains by addressing public service supply chain design, digitalization, and technology-enabled services. First, the study contributes to the debate on how public supply chains can use ICT and whether there are different levels of maturity, as often assumed. Most maturity models assume that digital transformation is the result of an ongoing progressive stepwise process towards advanced, fully integrated ICT (e.g., Andersen & Henriksen, 2006; Layne & Lee, 2001). In contrast, the present study finds that different supply chain designs with different kinds and usage of ICT exist for public services as a result of different performance aims, strategies, and approaches. Second, the study contributes to the literature by confirming that in a public service supply chain setting, technical, managerial, and political factors, similar to those observable in public intra-organizational settings, play a role. Third, the study shows that supply chain integration in this context only happens when explicit choices are made and procedures are adapted. Integration is certainly not an automatic result of the use of ICT, as is often assumed (Zhang *et al.*, 2011, 2016). In sum, this study advances the understanding of (public) service supply chains by means of its contribution to the understanding of why digital transformation in public service supply chains is so difficult. It shows the choices, dependencies, and complexities that governments and public bodies face, shedding light on the under-investigated field of digitally enabled supply chains in public settings. This helps to better understand how such service supply chains are designed and adapted. Its findings are also relevant for the use of ICT, and in particular inter-organizational ICT, in other (private) service supply chains. Also in these service supply chains, specific supply chain performance aims might require differential use of ICT and other ways of integrating partners in a chain; for example, a cost focus might require differences in both aspects compared to a focus on improved speed or delivery reliability.

## 3.2 | Theoretical background

As outlined in the introduction, the present study is fueled by several streams of research: public management, service operations management, service supply chain management, and information management. These are integrated into the study's research framework.

### 3.2.1 Characteristics of public service delivery processes

Public service organizations often operate collaboratively in order to achieve their purposes (Noordegraaf, 2016; Osborne *et al.*, 2012; Voets *et al.*, 2008), acting as a public service supply chain (Callender, 2011; De Blok *et al.*, 2015). For organizations within such chains, such as healthcare and justice organizations, it is necessary to exchange information extensively. Public service supply chains, as opposed to their private equivalents, can be characterized by their goals, i.e., they strive for equity in addition to effectiveness and efficiency, their political control structures, and their regulated processes. Moreover, public organizations have predetermined roles and responsibilities that are based in law (Andrews *et al.*, 2011; Berman, 2008;

Boyne, 2002; Bozeman & Moulton, 2011; Laing, 2003). These together with their diverse goals—equity, effectiveness and efficiency—mean that information in public service supply chains is judged on its availability, timing, and accuracy (Yang & Maxwell, 2011). In highly regulated supply chains, such as criminal justice supply chains, demands related to information exchange are even more important due to privacy, confidentiality, and authenticity concerns (Yang & Maxwell, 2011). These concerns stem from laws and formal policies that clearly define, and possibly restrict, conditions and processes for information collection and sharing, influencing the possibilities, the modes and intensity of information exchange (Dawes, 1996; Lam, 2005; Yang & Maxwell, 2011).

Taken together, the specific public performance requirements (i.e., efficiency, effectiveness, and equity), the regulatory environment (i.e., legislation and policies), organizational independence (i.e., differences in the goals, procedures, and rules of organizations, as set by government) and specific informational requirements influence inter-organizational information flows (Gil-Garcia & Sayogo, 2016; Lindgren & Jansson, 2013; Yang & Maxwell, 2011; Wenjing, 2011; Kuipers *et al.*, 2014). These factors might thus influence digital inter-organizational information flows as well as the implementation and utilization of inter-organizational ICT.

### 3.2.2 ICT in public services

Technological progress in ICT has changed service strategies by promoting the use of digital technology (Dunleavy *et al.*, 2006; Lindgren & Jansson, 2013; Lupo & Velicogna, 2018; Venkatesh *et al.*, 2012). Generally, in private-sector service supply chains, the effective flow of information across organizations is essential to support and manage key service delivery processes such as demand management, capacity management, and relationship management (Baltacioglu *et al.*, 2007; Ellram *et al.*, 2004) and thus to maintain inter-organizational performance (Ellram *et al.*, 2004). Ponsignon *et al.* (2011) identify service characteristics that should be considered for ICT-integration. These are: level of potential for automation; level of routine of activities; and connectedness of processes. Additionally, the study found that services with highly complex and variable inputs; with non-repetitive activities and tasks; and services with professional, customized outputs are harder to automate. These findings are specifically relevant for professional services such as consultancy and for public services such as healthcare and the justice system.

In public processes and management, ICT is supposed to lead to new and better service delivery by increasing efficiency and transparency, and by improving accountability (Cordella & Bonina, 2012; Cordella & Iannacci, 2010; Dunleavy *et al.*, 2006; Gupta *et al.*, 2008). Lindgren and Jansson (2013) stress that in order to ensure compliance with political policy and to ensure a shared sense of responsibility for the common public good, ICT needs to be steered by a formal, explicit, comprehensive, and stable set of rules. In addition, the extensive literature review by Yang and Maxwell (2011) provides a list of aspects (i.e., technological, managerial, and political) that influence the exchange of information across public organizations. Technological aspects relate to ICT adoption and the technological

capabilities of the parties involved and interoperability of systems. Managerial aspects are associated with, for example, differences in funding, control, and culture, degree of trust, (mis)alignment of interests, and (lack of) understanding of benefits of information sharing. Finally, political aspects include issues such as laws and regulations, requirements for confidentiality and security, and program and statutory boundaries. Because these factors influence inter-organizational information flows and thus likely also inter-organizational ICT, they must be taken into account when exploring the introduction of inter-organizational ICT in public service supply chains (Gil-Garcia & Sayogo, 2016; Yang & Maxwell, 2011).

To date, the complexity of the public inter-organizational ICT setting is not fully understood. Iannacci (2010, 2014) found that the use of ICT between public organizations (police and public prosecution) to exchange information digitally reduces administrative burdens and improves efficiency and effectiveness. However, these studies also concluded that, “keeping up with legislative and procedural changes considering that every time that there is substantial change in the law or in the organization of the criminal justice system, the criminal justice system exchange needs updating” (Iannacci, 2010, p. 42). To date, how public service supply chains that use inter-organizational ICT deal with legislation, procedures and complicating changes thereto, in combination with technological and managerial matters, remains unclear.

### 3.2.3 Inter-organizational ICT in public service supply chains

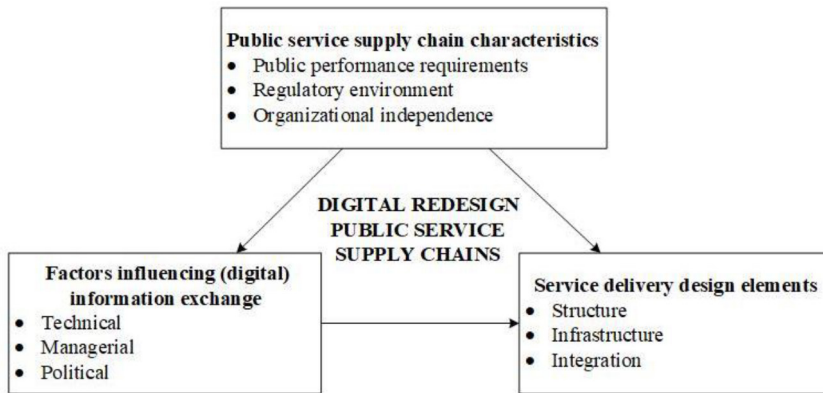
The use of ICT in service delivery processes has been empirically studied in general service settings (Ponsignon *et al.*, 2011) and public settings (Karwan & Markland, 2006; Iannacci, 2010, 2014). Both streams of literature identify criteria and aspects for consideration but lack a general overarching framework. It is clear that digital redesign and use of inter-organizational ICT in service settings are under-investigated. In addition, the significance of specific public-sector characteristics, as described in section 3.2.1, has not yet been fully explored.

In order to investigate digital public service supply chains, they are considered as service systems. The foundational work of Roth and Menor (2003) provides an exhaustive list of service delivery design aspects: structure (i.e., facilities, layout, technologies, and equipment), infrastructure (i.e., roles of service providers, people, policies, practices, processes, and performance systems), and integration (i.e., operations organization and coordination, service supply chains, integration technologies, and learning and adaptive mechanisms), which should be taken into account in the provision of the final service to the recipient (Machuca *et al.*, 2007; Meyer *et al.*, 2002; Roth & Menor, 2003). The service delivery system aligned with the service concept (i.e., what is offered to the service recipient) and target market requirements provides the basis for service delivery (Giannakis *et al.*, 2018; Machuca *et al.*, 2007; Meyer *et al.*, 2002; Roth & Menor, 2003).

The above discussion suggests that the interaction between public service supply chain characteristics (section 3.2.1), factors influencing inter-organizational ICT



(section 3.2.2), and service delivery design elements (section 3.2.3) shapes the digital redesign of public service supply chains. The nature of this interaction will be explored in the remainder of this chapter, as visualized in this study's research model, presented in Figure 3.1.



**Figure 3.1** Conceptual framework for digital redesign of public service supply chains

### 3.3 | Methodology

In line with the exploratory nature of the research, the present study applies a case study approach (Barratt *et al.*, 2011; Voss *et al.*, 2002; Yin, 2009) in order to facilitate an in-depth understanding of digital transformation in public service supply chains, specifically criminal justice supply chains. Because legal systems are rooted in the specific institutional context of their country, a cross-country multiple case study is performed. Details of the research setting, case selection, and methods of data collection and data analysis are presented in this section.

#### 3.3.1 Research setting

The criminal justice system can be described as the collection of institutions that together provide safety and justice to citizens and society as a whole (Callender, 2011; De Blok *et al.*, 2015). Within this system, the police, prosecution service, and courts work together closely to ensure the rule of law. Ministerial departments divide their budget between these organizations and are involved in setting their laws, procedures, and goals. This setting is appropriate for the present study for three reasons. First, criminal justice organizations collectively form a criminal justice supply chain, providing an inter-organizational public service setting. Second, because of the numerous and often complex interactions between organizations in this chain, the exchange of information between these organizations is especially critical. Accordingly, criminal justice supply chains have started to implement inter-organizational ICT, thus providing a setting in which digital transformation can be

observed. Third, in criminal justice, organizations must deal with high levels of political risks and legal regulations (Laing, 2003; Lindgren & Jansson, 2013) which is typical to a public service setting.

### 3.3.2 Case selection

To capture the inter-organizational nature of criminal justice, the national judicial system was selected as the study's unit of analysis. Within the range recommended for theory building by Eisenhardt (1989), four countries were selected that are considered by experts (as detailed below) to be front-runners in digital transformation and therefore should be suitable to provide valid evidence and facilitate solid conclusions. Based on publicly available information, countries were shortlisted for possible inclusion in the study that have indicated they are working on improving their systems by the use of inter-organizational ICT. These shortlisted countries were expected to have a high number of initiatives related to the implementation of inter-organizational ICT (Contini & Lanzara, 2009; Reiling, 2012; Velicogna, 2007), comparing to average countries. Additionally, ease of access of the countries in terms of distance and language, and the desire to achieve a certain geographically representative spread across Europe were considered. The shortlist of countries was discussed with experts in the field of criminal justice, and in consequence Austria, Denmark, England and Wales (hereafter, England) and Estonia were selected as the cases examined in this study. As indicated above, each of these systems is rooted in a different institutional setting, with rather different origins and historical development of the legal system (e.g., having a strong Roman system influence or not). To some extent, therefore, these systems are not comparable. For example, Estonia developed its current digital legal system rather recently and from scratch, whereas Austria began introducing digital technology in parts of its legal system relatively early (see Table 3.1). This study's focus is on the development of public-sector inter-organizational ICT systems, with an emphasis on public characteristics and achieving a well-coordinated overall service to the public, and it is submitted that such differences between the countries examined will be influential at the level of laws and legal procedures, but will not be of high importance for the design of digitally-enabled public-sector service delivery systems. Specifically, the justice organizations and related political entities involved in these countries' criminal justice supply chains play similar roles in their respective systems with similar types, characteristics, and limitations of information exchange in all countries investigated. Therefore, given the noticeable differences, it is submitted that the selected countries are an adequate sample for this study. Table 3.1 provides an overview of the countries' general characteristics, along with the nature of their plans and reasons for digital transformation.

**Table 3.1** Overview country-specific descriptive statistics and the nature of plans for digital transformation

	Austria	Denmark	England	Estonia
<b>Number of citizens*</b>	8,508,000	5,643,000	54,320,000	1,316,000
<b>Number of police personnel</b>	27,901	10,594	126,818	4,089
(Number per 100,000 citizens)**	(328)	(188)	(221)	(311)
<b>Number of professional judges or magistrates</b>	2,461	777	5,242	230
(Number per 100,000 citizens)**	(29)	(14)	(9)	(18)
<b>Number of criminal cases prosecuted</b>	279,818	410,809	1,458,915	8,710
(Number per 100,000 citizens)**	(3,285)	(7,275)	(2,541)	(662)
<b>Number of criminal cases convicted</b>	32,980	100,362	1,211,149	7,670
(Number per 100,000 citizens)**	(387)	(1,777)	(2,110)	(583)
<b>Government spending on public order and safety</b>	1.3	1.0	1.9	1.9
(Percentage of GDP)*				
<b>Start year (inter-organizational)</b>	1989	2005	2010	2004
<b>digital transformation in criminal justice system***</b>				
<b>Reason for digital transformation***</b>	Need for better working methods for justice professionals	Digital transformation of all governmental services	Budget cuts on organizational level	Transparency
<b>Main aim of digital transformation***</b>	Better support of the professionals working on criminal case files	Transfer information digitally	Increase efficiency within the criminal justice chain	Improved service delivery to customer-citizens

\* Statistics retrieved from Eurostat ([www.ec.europa.eu/eurostat](http://www.ec.europa.eu/eurostat)); data are for 2014, year of data collection. \*\* Statistics retrieved from united nations office on drugs and crime ([www.dataunodc.un.org](http://www.dataunodc.un.org)); data are for 2014, year of data collection. \*\*\* Based on desk research, documents, and interviews collected and analyzed for this study.

### 3.3.3 Data collection

For each country, data were collected from the three main organizations that work together in the criminal justice chain, being the police, the public prosecution service and courts, and the Ministry of Justice, as policy-making organization. Data collection included multiple sources of evidence to facilitate a process of triangulation and thus mitigate biases and enhance reliability and validity (Barratt *et al.*, 2011; Eisenhardt, 1989; Voss *et al.*, 2002; Yin, 2009). In total, 36 interviews were conducted, 39 relevant policy documents and reports on digital transformation initiatives were consulted, and 14 observations and multiple field visits were performed (see Table 3.2). The multiple case study comprised different stages of data collection. First, desk research was performed to provide country-specific information. Based on the findings, experts were consulted using semi-structured skype and telephone interviews in order to better understand each country-specific context and further develop the interview protocol. The main data, results of semi-structured interviews, and observations, were collected during visits of one week to each country between February and May 2014.

A total of 36 expert interviewees were carefully selected based on their ability to provide information on the criminal justice system from an organizational as well as a legal perspective, i.e., to understand both the judicial processes and how inter-organizational ICT is used to support this process. The interviews conducted face-to-face were organized at the interviewees' locations, mostly on an individual basis, with a few exceptions. Interviews lasted between one and two hours. Two researchers were involved in conducting each interview: one was leading the interview by asking the questions and probing to uncover insightful additional information, and the other took notes, ensured the interview was recorded, and asked additional questions when needed. All of these interviews were semi-structured and followed an interview protocol in order to facilitate data comparison and enhance internal and construct validity (Barratt *et al.*, 2011; Voss *et al.*, 2002; Yin, 2009). The interview protocol provided core themes and open-ended questions to explore digital transformation and enable detailed responses to be captured. Example questions were "What were the reasons to initiate inter-organizational ICT?"; "Which criteria, warranties, conditions, safeguards had to be taken into account?"; "What are the experiences with inter-organizational ICT in the criminal justice chain?" and "What are barriers and enablers concerning using inter-organizational ICT?" The interviews were transcribed and sent back to the interviewees for verification and confirmation of accuracy (Barratt *et al.*, 2011) and, when needed, were adapted based on comments provided. Despite the interviewers' efforts, it was not possible to interview all parties in all of the countries involved, but sufficient key informants were interviewed to provide suitable data for analysis. It was ensured to obtain an overall perspective on the criminal justice supply chain of each country by interviewing employees of the Ministry of Justice as well as project managers that were able to represent multiple parties. In addition, use was made of extensive documentation, representing the perspectives of the police and the public prosecution service and courts, which was added to the information

obtained from direct interviewees and enabled information saturation to be achieved in each case. Data triangulation was accomplished using 39 secondary documents, obtained via the Internet in preparation for country visits or provided by interviewees. These documents included management reports, project reports, strategy reports, and criminal procedures, all related to digital transformation in the criminal justice supply chain. Finally, 13 observations of both court hearings and ICT system demonstrations of between one and two hours were performed in order to get a hands-on understanding of the processes and practices within the criminal justice systems. In these events, audio recordings were prohibited, so only notes were made. These observations helped enhance understanding of the criminal justice system and inter-organizational ICT use in each of the countries, and ICT's implications in court.

**Table 3.2** Overview of interviews, observations, and documents

Data source	Organization	Austria	Denmark	England	Estonia	
<b>Interviews</b>	<b>Police</b>	-	ICT project manager	ICT project manager	ICT project manager	I.Es1
	<b>Public prosecution</b>	Senior public prosecutor	ICT project manager	ICT project manager	ICT project manager	I.Es2
		Senior public prosecutor	I.A1	ICT business consultant	Senior public prosecutor	I.Es3
			I.A2	Director Digital Business Program		I.En4
				Senior public prosecutor		I.En5
				Senior public prosecutor		I.En6
	<b>Courts</b>	President of Criminal Court	I.A3	ICT business consultant	Senior judge	I.En7
			I.D3	Senior judge	Senior judge assistant	I.En8
				Head of Criminal court	ICT project manager	I.En9
					Senior ICT advisor	I.Es7
<b>Ministerial department</b>		Project leader justice process automation	I.A4	Deputy head of Business Strategy	Head external relations ICT	I.En10
		Deputy head of legal informatics and ICT department	I.A5	Head of Digital Strategy department	ICT project manager	I.En11
		Head of legal informatics and ICT department	I.A6	Senior strategic advisor digital	ICT project manager	I.En12
					Senior ICT advisor	I.Es11
					Senior ICT advisor	I.Es12

**Table 3.2** Overview of interviews, observations, and documents (continued)

Data source	Organization	Austria	Denmark	England	Estonia	
Observations	Police	-	-	-	-	O.Es1 Demonstration ICT system
	Public	Demonstration ICT system	-	-	O.En1 Demonstration ICT system	O.Es2 Demonstration ICT system
	prosecution	Demonstration ICT system	O.A2			O.Es3 Demonstration ICT system
	Courts	Demonstration ICT system	O.A3 Court hearing	O.D1 Court hearing	O.En2 Court hearing	O.Es4 Demonstration ICT system
Documents			O.A4		O.En3 Court hearing	O.Es5 Court hearing
					O.En4 Court hearing	
		ICT project report	D.A1 Justice evaluation report	D.D1 Digital justice strategy report	D.En1 Digital justice strategy report	D.Es1 ICT project report
		ICT project report	D.A2 ICT project report	D.D2 Digital justice strategy report	D.En2 Digital justice strategy report	D.Es2 Justice strategy report
		ICT project report	D.A3 Ministerial note	D.D3 Justice strategy report	D.En3 Justice strategy report	D.Es3 ICT project report
		ICT project report	D.A4 Justice evaluation report	D.D4 Justice strategy report	D.En4 Justice strategy report	D.Es4 ICT project report
		Digital justice policy	D.A5 ICT strategy report	D.D5 Justice strategy report	D.En5 Justice strategy report	D.Es5 ICT project report
		Justice evaluation report	D.A6 Justice strategy report	D.D6 Justice evaluation report	D.En6 Justice evaluation report	D.Es6 Criminal justice procedures
		Digital justice strategy	D.A7 Justice strategy report	D.D7 Justice strategy report	D.En7 Digital justice report	D.Es7 Criminal justice procedures
		Criminal justice procedures	D.A8 Digital government report	D.D8 Digital government report	D.En8 Digital justice report	D.Es8 Criminal justice procedures
			Digital government report	D.D9 Digital government report	D.En9 ICT project report	D.Es9 Criminal justice strategy report
		Digital government report	D.D10 Digital government report	D.En10 ICT project report	D.Es10 Digital justice strategy report	
					D.En11 Criminal justice procedures	

### 3.3.4 Data analysis

The process of data analysis started with within-case analyses, followed by cross-case analyses (Voss *et al.*, 2002). In analyzing each case, case descriptions were made providing general insights on the strategies and performance aims, as summarized in Table 3.1. For the in-depth analyses of service delivery design considerations and influencing public factors, the interviews and documents were coded, which enabled data reduction and data categorization for each country's data (Miles & Huberman, 1994). The coding was performed independently by two researchers to ensure consistency and reliability. Subsequently, codes were discussed and adapted where necessary. Rather than using inter-coder reliability, suggestions from Gioia *et al.*, (2013) were followed and a focus was adopted on solving inconsistencies and differences between coders to make coding consistent and ensure validity. First, codes were assigned for service delivery system considerations (structure, infrastructure, and integration) (Roth & Menor, 2003) and influencing public factors (technical, managerial, and political) (Yang & Maxwell, 2011) to data items ranging from phrases to paragraphs (Miles & Huberman, 1994), guided by the study's theoretical concepts. Second, within each of these code categories, data items were coded using descriptive codes as first-order (within category) codes. Third, these first-order codes were grouped using interpretative coding to identify main concepts per category (Miles & Huberman, 1994). This provided coding categories consistent with the conceptualization of Roth and Menor (2003) and Yang and Maxwell (2011), as well as new categories (see Table 3.3 and Appendix 3.A). As such, the pattern coding reduced the data into smaller segments allowing for identifying within-case relationships between concepts and providing a starting point for cross-case analyses (Miles & Huberman, 1994). This resulted in in-depth case descriptions, which were compared and contrasted in cross-case analyses. In this cross-case analysis relationships were identified between design considerations and public factors, using the study's theoretical framework as a base. Analysis focused on similarities and differences in the digital transformation approach taken (i.e., the service strategy, the service delivery design considerations, and performance outcomes) as well as factors explaining the similarities and differences (i.e., instances and manifestations of different technical, managerial, and political factors), as summarized in Table 3.3. Although the interviews and documents were initially coded manually, all were subsequently entered into Atlas.ti software in order to facilitate the structuring and sorting of data segments and revision and reassignment of codes (Miles & Huberman, 1994).



### 3.4 | Results

The four countries investigated exhibit great differences in what they aim for and the reasons why they engage in the digital transformation of their criminal justice supply chains (see Table 1). These differences are reflected in decisions made concerning their digital transformation. Below, the results of the in-depth analyses of the four individual cases are presented, following the main theoretical constructs: 1) inter-organizational ICT introduced to serve the digital transformation and its main aims, i.e., *structural design decisions*; 2) changes made to existing processes, policies, and practices, i.e., *infrastructural design decisions*; 3) choices made regarding taking a supply chain approach to digital transformation, i.e., *integration design decisions*; and 4) public context factors, i.e., *technical, managerial, and political factors*. Sections 3.4.1, 3.4.2, 3.4.3, and 3.4.4 present the most important and characterizing elements for each country. Following the individual case analyses, section 3.4.5 provides a summary overview of similarities and differences between countries, supported by Tables 3.3 and 3.4.

#### 3.4.1 Digital transformation in Austria

Digital transformation in the Austrian criminal justice system mainly focused on supporting the work of law professionals: “by sending data electronically the exchange of information goes faster, there are fewer errors in the data, there is no need to re-enter data, et cetera. [...] We have to provide them [police officers, public prosecutors, and judges] solutions that are user friendly and time efficient” (Ministry of Justice, I.A5). Austria started the digital transformation process, (i.e., changing its service delivery *structure*) with the introduction of a government-wide (i.e., inter-organizational) electronic legal communication system which the police, public prosecution service, and courts use to digitally exchange procedural documents (D.A6). Two additional systems respectively support the electronic handling by the police and public prosecution of unknown offenders, and the automatic allocation of cases to public prosecutors and judges (I.A4). The case distribution system ensures accountability within the criminal justice system by ensuring a well-balanced and objective distribution of criminal cases across prosecutors and judges.

The existing *infrastructure* of the criminal justice supply chain is mainly preserved, for the reason that “it is not the purpose of the ICT strategy to change the criminal justice system” (I.A5). In fact, the decision “to replace paper processes with a digital way of working” (I.A5), resulted in a system that enables the digital exchange of information across organizations without changing underlying standards, procedures, or processes. Accordingly, related decisions involved changing the presentation of information and the way in which digital documents were used. Specifically, “we focused on how the criminal case file is built what the content of a file is and in what form the court needs to get the file e.g., electronically or paper-based” (I.A6). The criminal justice organizations and their professionals are provided the autonomy to create their own way of working with digital or paper documents.

In order to *integrate* the systems of the police, public prosecution service, and courts, a supply chain wide perspective was taken. “The aim is the development of a vision for the whole ICT landscape of the Austrian Justice System as well as the definition of the roadmap that is necessary for performing the redesign from as-is to to-be architecture under the given circumstances and in due consideration of trends. [...] avoiding island solutions” (D.A1). However, Austria is yet to achieve full digital inter-organizational information sharing because of the reliance on paper-based work routines. “It is not the whole case that is sent electronically, rather, documents from the police and the lawyers are received electronically by the prosecution. [...] The prosecution does not handle cases electronically; they print the documents and then they start building a criminal case file on paper” (I.A5).

*Technical factors*, mainly the low compatibility between intra-organizational ICT systems of various organizations influenced the inter-organizational digital transformation. Moreover, criminal case information is not yet suitable to be made digital because “the experience is that eighty percent of the steps that need to be taken to handle a large criminal file can be handled electronically, however for the remaining twenty percent this is not possible. You have to make a system which has the possibility for the electronic signature, which is not possible now” (I.A1). *Managerial factors*, i.e., the role, autonomy, and competences of professionals (public prosecutors and judges) induce resistance to change, and this influences infrastructural design decisions. As one interviewee stressed, “The judges still have a strong affection for their paper based files and therefore as a compromise, we had to settle for the future choice for the individual judge whether he wants to work on the digital based file, or on a paper based file” (I.A5). On top of the technical and managerial factors, *political factors* played a role. Necessary legislation and policies supported the implementation of inter-organization ICT and the use of digital documents across the justice system (D.A2; I.A6).

### 3.4.2 Digital transformation in Denmark

The use of ICT across Denmark’s criminal justice supply chain has been imposed by the national government, which has set a requirement for all governmental services to become digital (D.D9; D.D10). Digital transformation was aimed at creating digital instead of paper flows of information (I.D1). Concerning the changes in *structure*, an inter-organizational electronic communication system, ‘Datafolgesedlen’, was introduced to enable digital communication regarding procedural acts and exchange of procedural documents between the criminal justice organizations (I.D4). However, criminal justice organizations exchange criminal case files on paper, but intended at the time of data collection to connect their individual intra-organizational ICT systems in the near future.

There was great hesitation to redesign the *infrastructure*, for example, working processes, in order to make collaboration easier. Instead, parties within the system chose to digitize some working activities without changing working processes. In the future, Denmark intends to digitize criminal case information in accordance to the current method of presenting information. As an advisor of the Ministry of

Justice explained, “At this moment, we have a standard way how these cases have to be presented to the prosecutor. The standards prescribe which things have to be first and last” (I.D4). Similar standards are used for paper-based and digital criminal cases.

Concerning *integration*, at the moment of data collection, “the issue is that every authority is concerned about their small part of the chain and therefore does not feel the sense to contribute to other parts of the chain” (I.D6). To ensure criminal justice system-wide integration, the “Ministry of Justice launched in 2013 a number of initiatives for a consistent strategic focus on the criminal chain. Thus, the Ministry will strengthen transverse monitoring and multidisciplinary cooperation to support the Ministry of Justice and authorities” (D.D7).

The lack of integration can be explained by technical and managerial factors. Concerning *technical factors*, in the past each ICT project was generally approached from an intra-organizational perspective, explaining the lack of integration. The lack of compatible intra-organizational ICT systems caused the absence of secure digital information exchanges. Also, criminal case information is not yet suitable for digital transfer. Hence, criminal case information is printed, signed, and posted to the relevant parties. Concerning *managerial factors*, despite existing project teams that aimed to achieve supply chain wide digital transformation, a lack of supply chain-wide practices, experience and resources supporting collaborative work processes, coordinated decision making, and strategic connections is recognized by the organizations involved and by the Ministry of Justice. As indicated by an advisor at the Ministry of Justice, “most projects we have had were small projects within organizations, not cross-organizational” (I.D4). Concerning *political factors*, budgets were insufficient to cover the cost of digital transformation. Interviewees stated that ensuring public scrutiny was a challenge in the digital transformation, i.e., ensuring the transparency of the processes and decisions made in the system (D.D1).

### 3.4.3 Digital transformation in England

In England, fierce budget cuts had led to attempts to improve the cost-effectiveness performance of the criminal justice system. Consequently, the policies of the Ministry for Policing, Fire and Criminal justice and Victims aimed to achieve higher transparency, accountability, and responsiveness, while reducing costs. Redesigning the *structure* of the service supply chain focused on connecting intra-organizational ICT systems across organizations (D.En1; D.En2; D.En4; D.En5). For example, criminal justice parties communicate, exchange procedural acts, and exchange criminal case files from the police to the public prosecution service and to the courts digitally, enabled by a secure e-mail service. The individual intra-organizational systems of the police and the public prosecution service were connected, resulting in a bi-directional flow of digital information (I.En5). This enabled transferring up to date information on the defendant, victims, witnesses, and evidential material. In some courts digital criminal case files, sent by the public prosecution service, are used in preparation for and are consulted during court

sessions. At the time of data collection, design work had begun on a common ICT platform for the public prosecution service, defense parties, probation service, and the courts to access the case information provided by the police and to access, share, handle, and settle criminal cases to further improve the performance of the criminal justice supply chain (I.En12).

A key *infrastructural* design consideration in the introduction of inter-organizational ICT was the establishment of unified business processes. “You could just digitize a paper file, but actually we are more focusing on information that is in the paper instead of just transferring the paper file into a digital file” (I.En5). This process was motivated by three key concerns: “We are interested in looking at [1] the structured information of the document, [2] redesigning the use of this information, and [3] supporting the use of information by the professionals by information technology” (I.En5). Protocols were implemented to coordinate and standardize what criminal case file information is exchanged, in what form and when. These protocols streamlined the working processes within the criminal supply chain and helped to achieve coordinated information exchange.

In terms of *integration*, a supply chain perspective enabled the move “from a so-called ‘system’ which operated in silos [...] to a criminal justice service where police, prosecution, and courts work more effectively together. None of these reforms will compromise historic legal rights or important principles of justice. Rather the reverse: justice must be swift, sure, and seen to be done, or it is not done at all” (D.En5).

Concerning the contextual factors, *technical factors* helped to link the public prosecution system to each of the police forces, despite the fragmented intra-organizational ICT used by the police because “the 43 forces have their own budgets, systems, and suppliers” (I.En6). The public prosecution service designed a compatible system by making “it as open and generic as we [the public prosecution] possibly can. We connected our system to around 10 different types of police systems” (I.En4). *Regarding managerial factors*, the English criminal justice system can be characterized by regional and organizational differences in values and cultures related to resistance to change and concerns about losing autonomy. These differences were dealt with through leadership and project management based on experience, knowledge, and resources. Criminal justice boards, at both national and regional levels, were established. These consisted of senior managers from the different organizations across the (regional) criminal justice supply chain and related ministerial departments. These boards took leading roles to overcome fragmentation in the digital transformation of the criminal justice system (I.En2; I.En10). “Arrangements for coordination of agencies are increasingly open to local variation across the country. Local criminal justice boards still provide area-level coordination of local criminal justice partners.” (D.En3). At the *political* level, the use of inter-organizational ICT was steered by law-based values such as fairness of trials and independence of decision-making. At the same time, the case of England has shown that the parties involved reconsidered traditional practices. For example, “The actual ‘wet signature’ was not needed anywhere in that form. [...] We started

running digitally without any signed witness statements. And, so far, this has never been challenged” (I.En2).

### 3.4.4 Digital transformation in Estonia

The digital transformation of the Estonian criminal justice supply chain was primarily intended to increase the transparency of the criminal justice system for society, and to improve the accountability and accessibility for citizens, including defendants, victims, and witnesses (I.Es1; D.Es10). At the same time, the judicial and professional independence of professionals and criminal justice organizations were to be preserved (I.Es1; D.Es10). These aims were the cornerstone of the design of the *structure* of inter-organizational ICT. Pivotal to the transformation was the design of a central database that connected all individual intra-organizational ICT systems (D.Es1; I.Es3). Under the new system, the shared so-called E-file enables the criminal justice organizations to digitally exchange criminal case information and procedural acts, to manage the progress of cases and the allocations of caseloads between professionals, to monitor the performance of organizations, and to collect criminal justice system-wide management information (D.Es1; I.Es3).

A key *infrastructural* design consideration was the change of underlying procedures and processes to “create a harmonized business logic that provides guidance about how, when and what should and must be done” (I.Es9). More specifically, this included decisions on “how and what information should be entered in the E-file” as well as “who can start a criminal case, who can put in what information and who can access information” (I.Es9). “[Information] security classes are set [based] on availability, integrity, and confidentiality of information [exchanged]” (I.Es7). Additionally, in the system’s design, considerations included the presentation of information, the content of the information transferred between criminal justice organizations, and the assignment of roles and responsibilities (D.10). “The rules set by the Ministry of Justice provide requirements for the submission of data, composition of data, preservation of data, changing of data, and deletion of data” (I.Es7). Digital templates standardized the content and presentation of information (I.Es1; I.Es6).

In order to facilitate *integration*, i.e., to manage inter-organizational processes, the Ministry of Justice made use of system-wide management information. “All the developments and how to improve things, how to make it faster, how to narrow down the accessibility by different parties, all these things are done by the Ministry of Justice. Statistics, user feedback, different developments, analyzing the activities of the users, provides feedback to the Ministry of Justice” (I.Es11).

Related to *technical factors*, despite the existence of heterogeneous intra-organizational information systems, the compatibility of systems is relatively high. By use of the so-called E-file, the criminal justice organizations can communicate, exchange, and manage criminal case information. However, parts of the criminal case are not suitable for digital exchange. “We have the possibility to send all paper documents as an electronic file to the court via E-file. But there has to be a paper

document available according to law and therefore paper documents are used during court sessions" (I.Es3). Multiple *managerial factors* influenced the delivery system design in Estonia. Resistance to change, competing interests of criminal justice organizations, and organizational differences (I.Es7; I.Es10) were overcome because the government as well as the organizations in the supply chain had the required experience, resources, and knowledge to do so. In addition they benefited from appropriate leadership and project management (I.Es6; I.Es10). In order to implement the E-file system, multiple working groups were set up that involved users from criminal justice organizations, employees of involved Ministries, and information technology specialists (I.Es10). Regarding *political factors*, the use of inter-organizational ICT was positively influenced by rules and procedures set by law. "There were no laws that were blocking the design and development of the E-file system. The participants agreed that there was no need to change the law" (I.Es9). Generating transparency and accountability to the public provided several challenges to Estonian criminal justice. "There was a need to get more statistical information regarding the performance of the chain to be able to show the public how the system is performing and how the system works" (I.Es11). Yet this was overcome by introducing system-wide management information, which is communicated to the public, that served to increase public transparency. Also, citizens are able to access the E-file system through their own portal and obtain information on their proceedings and publically available information on judge's decisions on criminal cases, as well as other matters such as civil and judicial matters.

### 3.4.5 Summary

The detailed results of the individual case analyses are summarized in Tables 3.3 and 3.4. Table 3 shows how choices were made with regard to structure, infrastructure, and integration that are mainly explained by differences in terms of what each country aimed to achieve (Table 3.1). Choices resulted in ICT leading or following the wider design of the supply chain. In addition, Table 3.3 shows how digital transformation was affected by technical, managerial, and political factors. Table 3.4 demonstrates that different configurations of digital design are possible. It also shows that, in the end, none of the supply chains studied seek full digital information exchange encompassing all possible information.

Similarities between countries were mainly found in the factors influencing digital transformation, i.e., technical factors such as heterogeneous information systems; managerial factors such as organizational boundaries of bureaucracy, competing interests, different origins, values, and cultures, resistance to change, and concerns of losing autonomy; and political factors such as public scrutiny and judicial law-based constraints. Accordingly, it is found that managerial and technical factors do play similar roles to those they play in non-public contexts, in that incompatibility of ICT systems is a barrier. In addition, as is often the case in (albeit not limited to) public contexts, lack of leadership and expertise form another barrier, along with resistance to change and related issues. Choices and restrictions typical to

the public domain, such as budget constraints, public transparency, and political control, do also play a role in all cases. Specific to the judicial context, it is found that the use of inter-organizational ICT is limited by the nature of criminal law procedures that are necessary to ensure fair trials (I.A3, I.En2). “[We have to deal with] the equality of the prosecutor and the defendant. The prosecutor, by law, is not allowed to have advantages in comparison to the other party concerning presenting or defending the case” (I.A3). Also, judicial independence of the courts provides challenges to transforming the criminal justice supply chains to digital ones (I.D6; I.Es7).

Differences between countries on design considerations and influencing factors (marked grey in Table 3.3) provided two interesting insights. First, despite all cases aiming for a service supply chain orientation, Table 3.3 highlights that England and Estonia adapted both their inter-organizational structure and infrastructure, whereas Austria and Denmark aimed more to fit structural components to the existing inter-organizational structure and infrastructure. These differences in approaches and outcomes are consequences of political and judicial, law-based choices regarding performance outcomes of the service supply chain, and interpretation of, for example, what independence of different powers in the judicial system should mean. Second, cases show differences in the final design of the digital criminal justice supply chain (see Table 3.4). More specifically, in all cases paper-based files are still used in court, due to specific criminal justice related factors such as the independence of the courts and the equality needed between prosecution and the defending party.

**Table 3.3** Service delivery design elements and influencing factors per country

	Austria	Denmark	England	Estonia
<b>SERVICE DELIVERY DESIGN ELEMENTS*</b>				
<b>Structure</b>				
Technology supporting:				
<i>Criminal case registration</i>			X	X
<i>Criminal case distribution</i>	X			X
<i>Criminal case exchange</i>			X	X
<i>Criminal case management</i>			X	X
<i>Chain-wide management information generation</i>				X
<i>Digital Communication</i>	X	X	X	X
<i>Criminal case (procedural) information exchange</i>	X	X	X	X
<i>Inter-organizational ICT supporting one-way transfer</i>	X	X	X	X
<i>Inter-organizational ICT supporting two-way transfer</i>			X	X
<b>Infrastructure</b>				
(Re)design people			X	X
<i>Redesign how people use the information</i>			X	X
(Re)design policies and procedures			X	X
(Re)design practices			X	X
<i>Redesign and standardize the presentation of information</i>			X	X
<i>Redesign the use of information</i>				
(Re)design processes			X	X
<i>Redesign how information is transferred</i>			X	X
(Re)design performance systems				
<b>Integration</b>				
<i>Supply chain perspective to justice system</i>	X		X	X
<i>Alignment through use of chain-wide management information</i>				X
Integration technologies	X	X	X	X

X = present; | = not present; + = positive influencing factor; - = negative influencing factor

\*Italic presented codes are inductive codes; non-italic presented codes are deductive codes



**Table 3.3** Service delivery design elements and influencing factors per country (continued)

	Austria	Denmark	England	Estonia
<b>INFLUENCING FACTORS ON DIGITAL TRANSFORMATION*</b>				
<b>Technical</b>				
ICT capability	-	-	+	+
<i>Compatibility of systems</i>	-	-	+	+
<i>Suitability of criminal case information to become digital</i>	-	-	+	+/-
<i>Synchronization of paper and digital information flows</i>	-			
Heterogeneous information systems	-	-	-	-
<b>Managerial</b>				
<i>Leadership and project management</i>	+	-	+	+
Experience	-	-	+	+
<i>Resources and knowledge</i>	-	-	+	+
Organizational boundaries of bureaucracy	-	-	-	
Competing interests	-	-	-	-
Different origins, values, and cultures	-	-	-	-
<i>Regional differences</i>	-	-	-	
<i>Organizational differences</i>	-	-	-	-
Resistance to change	-		-	-
Concerns of losing autonomy	-		-	
<b>Political</b>				
Legislation and policies	+	-	+	+
<i>Budget</i>	+	-	+	+
Public scrutiny	-	-	-	-
<i>Equality of prosecuting and defending party</i>	-	-	-	-
<i>Judicial independence of courts</i>	-	-	-	-

X = present; | = not present; + = positive influencing factor; - = negative influencing factor

\*Italic presented codes are inductive codes; non-italic presented codes are deductive codes

**Table 3.4** Digital redesign of criminal justice supply chains per country

	Austria	Denmark	England	Estonia
<b>Extent of digital transfer of procedural information and documents</b>	Fully digital	Fully digital	Fully digital	Fully digital
<b>Extent of digital transfer of criminal case information and documents</b>	Partly digital, partly paper-based	Partly digital, partly paper-based	Fully digital	Fully digital
<b>Mode of use of criminal case in court</b>	Fully paper-based	Fully paper-based	Both digital and paper-based	Both digital and paper-based

### 3.5 | Cross-case analysis and discussion

From the results and comparisons presented in Tables 3.3 and 3.4, two interesting themes emerged. First, related to the main research question, the study detects two possible approaches towards (re)designing public service supply chains into digital systems: digitization and digitalization. Specifically, as further discussed in section 3.5.1, it is found that not being ‘fully’ digital might be an appropriate solution for (legal) public service supply chains. Second, the study facilitates better understanding of how service delivery design elements, i.e., the use of inter-organizational ICT, and integration are related, as further discussed in section 3.5.2. It is found that decisions related to using inter-organizational ICT and applying integration practices are distinct and consequently affect the configuration of the digital design differently. The study distinguishes different mechanisms and configurations of integration and inter-organizational ICT that are related to the focus on one or several public service performance aims.

#### 3.5.1 Digitization and digitalization in a public context

This study’s findings show that countries approached the structure and infrastructure of their service supply chains in different ways. Austria and Denmark, on the one hand, took the *structure* of the service supply chain as a starting point and implemented inter-organizational ICT that enables digital exchange of information. Whenever they came across incompatible systems or processes between organizations they started adjusting them, within the relevant restrictions imposed by laws, regulations, and procedures. On the other hand, England and Estonia adapted the *infrastructure* of the service supply chain before the structural elements related to inter-organizational ICT. Laws and procedures were adapted accordingly or interpreted in a more flexible sense to enable digital transformation. Both types of approach also had different aims: Austria and Denmark focused on more efficient information exchange across organizations, while largely maintaining existing professional autonomy. Although efficiency also was a goal for England and Estonia, transparency and quality were as well. These performance aims induced the use of digitalization to connect professionals and professional organizations, creating technologies that support digital information exchange and digital working, while preserving the independence of organizations. Taken together, two different approaches are identified, one can be labelled as digitization (Austria and Denmark) and the other as digitalization (England and Estonia). *Digitization* directly converts physical flows of information into digital flows, mainly redesigning the modes of input and output of the service supply chain. In contrast, *digitalization* redesigns processes, procedures, and practices, in addition to redesigning the modes of input and output, to fit the support functionality of digital systems and technologies.

Interestingly, both digitization and digitalization enable digital exchange of information, but require different adjustments in the structure and infrastructure of the service supply chain. It is found, however, the one is not inherently better than the other. This is in contrast to what has been suggested in conceptual

literature related to e-government maturity models (Andersen & Henriksen, 2006; Iannacci *et al.*, 2019; Janowski, 2015; Layne & Lee, 2001). Generally, such models assume that digital transformation is the result of an ongoing progressive stepwise process starting with use of simple ICT and progressing to completely integrated, advanced, and all-embracing ICT, resulting in improved performance outcomes (e.g., Andersen & Henriksen, 2006; Layne & Lee, 2001). Within such a perspective, digitalization is presented and perceived as more advanced, or more mature, and seemingly more evolved than digitization (Gottschalk, 2009; Janowski, 2015; Sandoval-Almazan & Gil-Garcia, 2018). However, this study's results show digitization and digitalization to be the outcomes of deliberately made choices. For example, Austria applied partial integration in order to preserve professional independence and judicial traditions, as well as to preserve the performance aims of the service supply chain. These are all embedded in the political decision-making process and the public and country-specific institutional setting. Not being 'fully' digital might thus be an appropriate solution for any public service supply chain. Therefore, in line with Osborne (2010) and Osborne *et al.* (2012), it is argued that policy makers should explicitly consider what outcome they aim to achieve when making changes in a public service supply chains. Understanding the institutional setting, setting aims for the public and users of the chain, and setting priorities with regards to costs, transparency, or equity might result in different decisions regarding the structural and infrastructural decisions and thus the digital design. Although this might sound obvious, in the ICT field in particular, there remains a strong belief in maturity models when considering digital transformation of public services. A change in this perspective may be beneficial not only for governments but also for researchers.

### 3.5.2 Integration and ICT

The study's findings provide additional insights into how service delivery design elements, i.e., the digital structure (i.e., the use of inter-organizational ICT) and integration, relate. It is found that the decision to integrate and the decision to use inter-organizational ICT are not one and the same, and this distinction has implications for the configuration of the digital design.

First, earlier research in physical, product-oriented settings shows that there is some belief that implementing ICT in a chain improves the coordination and integration in the chain (Zhang *et al.*, 2011, 2016). In contrast, it is found that integration and the use of digital structures and infrastructures have a more complex interrelationship. Although the aim to digitally transform can motivate the integration of different organizational processes involved in the public service supply chain, as in England and Estonia, this is not a necessary prerequisite of digital transformation, as the cases in Austria and Denmark show. It is thus found that the decisions related to integration of processes and the use of inter-organizational ICT in the context of digital redesign are separate ones. It is not necessary to consider both, or to consider them at the same time.

Second, it is found that the relationship between integration, the use of inter-

organizational ICT, and performance is not straightforward. Although integration and the use of inter-organizational ICT might be mutually supportive, it is hard to identify the performance levels achieved in any of the cases as being inherently superior to others. This contrasts somewhat to the findings of Karwan and Markland (2006) who find improvements in both efficiency and equity attributable to *intra*-organizational ICT. This study's results indicate that, in line with Zhang *et al.* (2011, 2016), the mechanisms for intra-organizational and inter-organizational ICT and digital transformation might be different. Apparently, performance outcomes related to digital transformation of the chain using inter-organizational ICT seem to depend on the interplay between the public aims chosen, the level of integration between organizations and their processes, and the choices for the type of inter-organizational ICT introduced. This can be illustrated by three different configurations found regarding inter-organizational ICT and integration. First, in Austria and Denmark it is found that inter-organizational ICT efforts are aimed at achieving performance improvement without adapting or improving inter-organizational processes and their integration. Second, in England and Estonia inter-organizational processes and integration are adapted to enable inter-organizational ICT implementation, and in so-doing, also performance improvement. In these two cases, ICT efforts entailed alignment of inter-organizational processes to facilitate information exchange. Third, in Estonia a distinguished effect is found, as inter-organizational ICT is used to achieve even higher levels of integration, i.e., more aligned processes and smooth information exchange. Specifically, Estonia used ICT to generate supply chain-wide management information that then was used to improve coordination along the chain.

Overall, it is shown that the application of inter-organizational ICT, i.e., the creation of a digital structure and infrastructure of supply chains, does not automatically result in changes in the integration and coordination of the chain, nor the other way around. Therefore, inter-organizational ICT in public supply chains, such as those of criminal justice systems, might influence supply chain performance via different mechanisms, i.e., having a direct relationship or having an indirect relationship in which integration may play a mediating or moderating role (Zhang *et al.*, 2016, 2011). To a large extent the different configurations observed in this study's cases are shaped by the focus on one or more of the typical public-sector performance goals, such as equity, efficiency, and effectiveness. Therefore, it might be that these configurations are typical for the type of public service supply chains investigated in this study. An interesting avenue for future research may be to investigate whether such different configurations can also be found in other chains, in both the public and private sectors, and to what extent such configurations depend on similar or different specific goals. Amongst profit-oriented supply chains, it might be interesting to investigate whether the pursuit of goals related to environmental sustainability issues such as the environmental impact of the supply chain also leads to different configurations of supply chain integration and ICT, as compared to ordinary profit-oriented supply chains.

### 3.6 | Conclusion, managerial implications, and future research

This study aimed to explore how public service supply chains (re)design their joint service delivery processes when introducing digital processes. Accordingly, the study aimed to advance the understanding of service supply chains by addressing public service supply chain design, digital transformation, and technology enabled services. This study found two types of digital transformation, i.e., digitization and digitalization, which reflect different service supply chain approaches as a result of different public service strategies and objectives (i.e., efficiency, effectiveness, and equity) as well as institutional and political differences in emphasis on specific public service characteristics (i.e., separation of powers and autonomous professionals). Comparable to non-public settings (Barratt, 2004; Richey *et al.*, 2010) technical and managerial factors provided enabling and constraining factors for the implementation of inter-organizational ICT, along with factors specific to the public-sector such as constraints in budgets and political control of implementation. Finally, although service supply chain integration is often aimed for, improving such coordination along the service supply chain requires more than implementing ICT. Overall, this study contributes to the under-investigated field of digitally enabled supply chains in public settings and help to better understand how such service supply chains are designed. Additionally, in for-profit service supply chains, the specific performance aims of the supply chain might require differential use of inter-organizational ICT and other ways of integrating partners in the chain, e.g., a cost focus might require a different use of these factors as compared to a focus on improved speed or delivery reliability.

#### 3.6.1 Managerial implications

The present study helps to understand the complexity of digital transformations and the challenges politicians, policy makers, and public managers face, but also provides insights into how to possibly handle this complexity. The results clearly show that there are multiple ways to redesign public service supply chains into digital ones, and the process of such a redesign starts with clearly articulating policy choices and priorities. Regrettably, digital transformation is often pictured as a straightforward road to overall service performance improvement and lower costs. Based on this study's results, it is submitted that digital transformation should actually start with a reconciliation of aims and service delivery attributes that considers the desired traits of economic, social, and political performance (West, 2004).

Politicians, policy makers, and public managers should regard the use of inter-organizational ICT as a means to an end. A starting point in public service supply chain redesign might be to articulate which aspects of the public service will be changed, what budget is available, and consequently to rethink the consequences for the design of the overall service supply chain. In this process, existing laws, procedures, public norms, and traditions need to be considered in order to prevent likely failure. Unfortunately, there is ample evidence of such failure not only in

criminal justice service supply chains, but in general governmental and public-sector ICT projects (Karwan & Markland, 2006; Venkatesh *et al.*, 2012). Based on this study's findings, for digital transformation in complex service supply chains an approach is recommended that reconciles both the public element and the supply chain aspects of the service. Additionally, as is the case in any large project, but, due to public factors as accountability, political influence and regulations especially important in the public context, managerial and technical means need to be adequate for the process.

In line with the above implications, politicians and public managers should be realistic in their promises and communications with respect to the level and nature of improvements in this context. This study's findings provide examples of both overpromising—in Denmark the ambition to become fully digital and the available means did not yet align—and realism—Austria set limited, realistic expectations for the public with a focus on professional and judicial traditions in digital transformation, and met these expectations successfully.

### 3.6.2 Limitations and future research

As with all research, this study has some limitations. First, this study's findings mainly build on interviews with non-users of the supply chains studied, such as ICT project managers and policy makers, and on strategic and project related documents instead of system users such as police officers, public prosecutors, and judges. However, the study aimed to investigate design considerations associated with digital transformation in public service supply chains and related influencing factors, but still the views of users and service beneficiaries could have added to our insights.

A second, related, limitation is this study's focus on the three main actors of the criminal justice system, i.e., police, the public prosecution service, and courts, excluding other users such as the probation service, imprisonment system, lawyers and solicitors, or the impressions held by society in general. Although the inclusion of such actors is of interest and merits further study, the present study opted to focus on the three core actors and their inter-organizational service delivery. These three organizations provide the backbone of the criminal law supply chain and fitted best with this study's focus on inter-organizational design of the digital service supply chain. However, further research should also examine the perspectives of all different users and their perceptions of service supply chain benefits or restrictions. In the unique cross-country comparison performed by the present study, including such a diversity of perspectives was virtually impossible and beyond the study's main goals.

Third, related to the above, the effects on public service performance levels were not considered, despite performance improvement being a primary aim of inter-organizational ICT implementation (Karwan & Markland, 2006; Kocabasoglu-Hillmer *et al.*, 2019; Zhang *et al.*, 2011, 2016). As indicated, the present study aimed to understand choices involved in the digital transformation in public service

supply chains. Despite the known difficulty in so-doing, future research should aim to measure and understand the mechanism of performance improvement by means of inter-organizational ICT in public settings. It is submitted that the present study's findings are supportive for this kind of study.

Fourth, the present study did not explicitly consider integration practices, although some results show their important link with digital transformation. It is found that the relationship between inter-organizational ICT, integration, and performance is not straightforward. Investigating this relationship offers another interesting avenue for further research, both in the service supply chain domain and in the public service domain, given both have distinctive characteristics and barriers to integration. In line with the preceding discussion, it is suggested that future research should study integration mechanisms together with public digital service delivery system design in more depth.

Finally, the use of ICT is approached in this study from a service supply chain design perspective (Roth & Menor, 2003) to understand the relationship between design choices and outcomes. Another approach is suggested by Mignerat & Rivard (2009) considering the introduction and utilization of ICT from an institutional theory perspective. Under this approach, different alternative lines of research and analysis of the processes described in this chapter then emerge, such as understanding the institutional pressure to implement ICT, which might partly stem from new public management approaches designed to mimic for-profit companies. Another possible perspective is to focus on the interaction between ICT and the institution, with reference to the interrelated institutionalization processes that play a role in the development of both ICT and new organizational processes (Mignerat & Rivard, 2009).

## Acknowledgements

This study built on the data gathered in the project 'Digitalisering in strafrechtketens' (Digitization in criminal justice chains) commissioned by the Dutch Ministry of Security and Justice, WODC. We acknowledge the contributions of prof. dr. Rinus Otte, LL.M., prof. dr. Berend Keulen, LL.M. and Inge Schaafsma-Roukema, LL.M. to the data gathering and initial interpretation. In addition, we would like to thank the reviewers and Guest-Editors for their constructive comments.

## APPENDIX 3.A: Excerpt of coding including all categories on service delivery design consideration and public factors

First order codes	Service delivery system design considerations	Type of design consideration
Electronic legal communication with the courts has worked extremely well since its introduction in the year 1989. However, the electronic transmission of original documents and attachments to submissions to the courts in electronic legal communication has not been possible so far. (DA6)	Criminal case communication	Structure
e-Filing with the courts as an instrument of communication with the parties of proceedings, on the same level as paper, was introduced in 1990. As far as it is known the Austrian administration of justice is the first country that has introduced e-filing, e-Filing and e-Delivery in legal relations allows electronic transmission of applications or submissions and the automatic transfer of procedural data to the Automation of Court Procedures. (DA6)		
The interaction with other parties than the police is not always digitally. As far as digital is concerned, it is primarily using email to exchange information. [...] It is a modern post transport mechanisms instead of a way of digital working. (LEn5)		
All the documents we have in the E-file system is used as a basic background on the status of the case until the police has finished their investigation. [...] To make sure the system works and supports the work of criminal justice system all documents and all decisions need to be registered in the system. (LEs3)	Criminal case registration	
As a result of the first project phase all proceedings concerning unknown offenders (about 2/3 of all proceedings) are managed via EIIAs. Incoming charges generate EIAs files which are then presented to the federal or district prosecutors. Using simple menu navigation prosecutors may about the proceeding according to § 197 StPO (code of criminal procedure) in an electronic (paperless) way (about 90 % of actions concerning unknown offenders). Currently other constellations are handled by means of paper files. (DA6)	Criminal case (procedural) information exchange	
When for example a witness is heard by the police, the witness needs to sign the document including his statements. This document is either scanned or written in for example word, so that the information can be transferred to the prosecution service digitally. However, it might be that the sign of the witness is not there. Nevertheless, the original paper file is stored at the police, so it could be requested. This does not lead to any problems. (LA4)		
This means, today, that criminal cases are handled manually to a large extend. In 2006, the authorities decided to develop a temporary solution 'Datafolgesedle' (data delivery note). This solution was only meant to be temporary as it only increased efficiency marginally. It is still based on copying and re-entering data and does not contribute substantially to the turnaround time and incorrect administration. Moreover, it only covers a few steps in the criminal justice chain and it is not even implemented in all local authorities. (LD4)		
If you want to take a suspect into custody, the court provides permission via the system. For example, whenever I have a court case going on and the first instance court has made a verdict and I want to appeal than I, as a prosecutor, sign the appeal with a digital signature and send it to courts using the E-file which automatically comes into the system of the courts. (LEs3)		



Structure	Criminal case distribution	
		<p>It is also possible to divide court cases automatically to judges - KIS offers complicating system that provides equal and random allocation. There are two ways to allocate court cases: automatically – judge is chosen by system; and manually – court official can choose between various judges. (D.Es1)</p> <p>There is also a new automated court case dividing system, that take into consideration case type, capacity of case, workload on the judge etc and based on that information the system will automatically decide which judge will get which case. (D.Es1)</p> <p>Right now the judge can easily get an overview of his case from KIS, also judge can examine other cases, plan court hearings and etc. Court officials can generate court summons, look up for participate contact details, bring into force judgements and publish them to public or to the parties via the Public e-File. (D.Es1)</p> <p>The E-File is a central information system currently being developed (to be implemented in 2011), which is going to provide an overview of the different phases of the criminal, civil, administrative and misdemeanor procedures, procedural acts and court adjudications to all the parties involved. It is an integrated system for proceedings, which enables the exchange of information simultaneously between different parties. (D.Es4)</p> <p>Prosecutors the E-file client system as an information system but also as a communication system. For example, if a prosecutor needs to ask permission from the court, for example to tap a phone, the request is put in the system while adding the digital files that are required to get the request approved. (LEs3)</p> <p>The development of datafolgesedlen step 2 is that you can send documents directly to the court's case system, in their back office behind the firewalls and vice versa. (LD1)</p> <ul style="list-style-type: none"> <li>- data entered in Police Info System is simultaneously accessible by a prosecutor in the prosecutors' Register;</li> <li>- information can be further used and changed by the prosecutor in the prosecutors' Register and sent to the KIS; - procedural information and the court decision entered into force, could be delivered to the Prison info system, etc. (D.Es1)</li> </ul> <p>Around 2005, they started synchronically data exchange. The data was one-directional from the police to the prosecutors. Some of the case data went synchronically from the police information system into the prosecutors information system. Before, the data exchange was only one directional, so if the prosecutor made some changes/corrections or proceedings, then the police could not get this information back using the information system. (LEs9)</p> <p>All police systems are connected directly to the prosecution service. They can all exchange documents the prosecution service. Some of the police forces use a one-way information, only enabling to send information to the prosecution service, some of the forces use two-way information, so that they can receive information from the prosecution service digitally and directly as well. (LEs5)</p>
	Criminal case management	
	Criminal case exchange Criminal case management Inter-organizational ICT supporting two-way transfer	
	Criminal case communication Criminal case (procedural) information exchange	
	Inter-organizational ICT supporting one-way transfer	
	Inter-organizational ICT supporting two-way transfer	

Infrastructure	Redesign and standardize the presentation of information	National File Standard is a result of the work of the National Prosecution Team, police and CPS. It is basically saying in relation to a particular type of case, which points in the case's life cycle are required for the case evidence. It is expressed in documents and forms. However, we expect not to see a physical file, but a digital file. There is actually work at the moment to reduce the amount of information in the file, the police is sending too much. So there is work underway to do to help the police in designing a new file. It should be a very short document that sets out what the case is, highlights bits of the evidence, and is intended for those cases when the police knows the defendant is likely to plead guilty. (LEn6)
	(Not) redesign how people use the information	The employees of the judiciary should continue in their duties by specialized custom applications or where possible and be usefully support automation. - A judicial wide transaction processing to each organizational unit Make (or person or) electronically accessible in the judiciary (Similar to email) and with high integration capability. (DA7)
		The judges still have a strong affection to their paper based file, and therefore as a compromise we had to settle for the future choice for the individual judge whether he wants to work on the digital based file, or on a paper based file. With one exclusion, if he chooses to work on a paper based file exclusively, nevertheless he will provide a complete digital copy of the paper file. (LA5)
		On local level, courts and police districts agreed on: if they use it, when they use it and for what. Within the courts and police offices is also described how they use it. At the moment, there is no date set from when the use of Datafölgesseden will be mandatory. (LD1)
		The collection of information by the police is based on requests where the system tells them what information to put in, instead of putting together one story about the case (lacking part of information or with no standard structure). (LEn5)
	(No) redesign processes	The Police did not take advantage of the opportunity to rethink and streamline business processes and procedures, but decided that the POLSAG system should resemble the existing IT system. (DD1)
		We have learned to start with improving the processes in terms of efficiency before designing the system that supports the processes. We have learned from the previous project of MIS that digitizing a bad process results in a bad digital process and therefore with the third version of MIS we aim to improve processes and its efficiency. (LEs1)
	Redesign policies and procedures	With these regulations we have established the rules for example we have regulated how the submitting the documents to the courts. For example we have regulation how the electronic submitting is regulated and rules about the court information system etc. (LEs6)
		As a result of police officers increasingly capturing information in a digital format, the digital streamlined case file project will seek to make sure that clear guidance is in place for prosecutors about what should be included in the case file when they go to Court. (DEn1)
		There is the program 'the streamlined digital file' from the national prosecution team leading, which means effectively defining for each offence type what the information requirements are. This will ensure that the forms will provide a guidance to fill in based on the type of offence. (LEn11)

Infrastructure	Redesign practices	
Integration	Supply chain perspective to justice	<p>It was the way of exchanging information that changed. Each of the organizations needed to develop new (upgraded) systems to be able to connect to the e-file. Because otherwise the systems were not able to the e-file system. (l.Es9)</p> <p>Central to this is the proposal to establish a streamlined digital case file. Creating a digital file at the outset will save the police time which is currently spent creating paper files, as well as reducing considerable work further down the line for the prosecution, defense and court staff. It will also ensure all case files are created to the same standard, which will assist officers to provide just the required information but no more. (D.En2)</p> <p>The aim of the strategic initiative „Justiz 3.0“ is the development of a vision (to-be architecture) for the whole IT landscape of the Austrian Justice System as well as the definition of the roadmap that is necessary for performing the transformation from as-is to to-be architecture under the given circumstances and in due consideration of trends. (D.A1)</p> <p>One solution for all courts and types of court proceedings – Coordination and prioritization of requirements – Avoiding of „island solutions“ (D.A1)</p> <p>Ministry of Justice launched in 2013 a number of initiatives to ensure a consistent strategic focus on the criminal chain. Thus, the ministry will strengthen the transverse monitoring and multidisciplinary cooperation to strengthen the ministry and authorities. (D.D7)</p> <p>The issue concerning this is that every authority is concerned about their small part of the chain and therefore does not feel the sense to contribute to other parts of the chain. (l.D6)</p> <p>The e-file system is used for the criminal justice system, but also other justice systems are able to use the e-file system to exchange information. [...] We have the central system, connected to the police system, the criminal case management system, the system for prosecutors, the court information system, the management system, the supreme court and the statistic management system. (l.Es9)</p> <p>Simple errors at the outset of a case can lead to substantial re-work further down the line and trials not taking place on the day they were scheduled or even collapsing. Making sure that the case file has everything it needs and nothing it doesn't is crucial – with the right information available at the right time, to ensure appropriate pleas can be entered at the earliest stage possible. [...] Working in partnership: we simply cannot continue with a situation where one part of the system routinely operates in a way that causes problems for another. Nor can we continue to procure incompatible IT systems or take decisions about the location of estates without thinking about the impact this has on the overall CJS landscape. [...] This Strategy and Action Plan starts from a simple premise that all parts of the CJS should be working towards achieving the same set of outcomes. (D.En2)</p>

Integration	Supply chain perspective to justice	
		Alignment through use of chain-wide management information
	<p>Delivery partners need to work well together at national and local level, focusing on how best to achieve the overall objectives of the System, rather than optimising the performance of their own organisations. The need for good local joint working is even more crucial in the light of changes to local accountability and performance measurement. [...] Since the last general election there have been significant changes to the governance of the System. Recognising the need for joint working, the government appointed a Minister of State for Policing and Criminal Justice, who reports to both the Secretary of State for Justice and the Home Secretary. Joint governance structures are also in place, primarily a Criminal Justice Board (the Board), to provide accountability and coordination across the System and help overcome operational barriers. The Board comprises ministers and representatives from the Ministry, the Attorney General's Office, CPS, the Home Office, police and victims. It is intended to set the direction for how criminal justice partners work together. (DEn3)</p>	
	<p>From a so-called 'system' which operated in silos, we are moving to a criminal justice service where police, prosecution and courts work more effectively together. None of these reforms will compromise historic legal rights or important principles of justice. Rather the reverse: justice must be swift, sure and seen to be done, or it is not done at all. (DEn5)</p>	
	<p>Having the joint minister made it possible to join up the home office and the ministry of justice and therefore to join up the parties across the criminal justice system. The joint minister and the joint CJS board make the system more accountable. It is the constitutional independence of the different parts of the system is seen by the public as one system and therefore we have to act as one system where different parts are responsible for each other. (LEn12)</p>	
	<p>The ministry of justice is the owner and controller of the e-file system. So all the developments and how to improve things, how to make it faster, how to narrow down the accessibility by different parties, all these things are down by the ministry of justice. Statistics, user feedback, different developments, analyzing the activities of the users, provides feedback to the ministry of justice. (LEs11)</p>	

First order codes	Influencing factor	Type of influencing factor
<p>Harmonizing systems and equipment, electronic document archive, links to applications Integrating additional secure features (e.g. Digital Signature) (DA3)</p> <p>One of the problems is that the IT support in the police is much less developed than in the prosecution and the courts. ... We should be on the same level and we are not. They are below our level in terms of technical equipment, IT support. (IA3)</p> <p>The systems between the different justice parties are not combinable. The police have other systems than the court and the prosecution. The police sends information electronically to the prosecution, however the prosecution office uses other systems and therefore information needs to be inserted manually in the prosecution system. (IA2)</p> <p>Also the rigsvisionen had difficulties to oversee the whole chain. Because all organizations have different systems/data and different ways to read it, different definitions. (LD4)</p> <p>Because all organizations have different systems/data and different ways to read it, different definitions. (LD5)</p> <p>For designing the e-file system we used a domain-driven design approach, we used typical data driven development techniques. All the data is exchanged using the x-road. We have four layers in the e-file system. The x-road is the adapter which receives the xml formatted queries. The next layer is the web layer. It converting into the domain and forwards them to domain services. The third layer business logic is situated for each business logic service there is one domain service class. The fourth layer is the database layer exchanging information between domain layer and database. All inquiries towards to database goes only through this layer. (LEs9)</p> <p>It is essential to retain the independence of operational policing and prosecutors, courts, defence and judiciary in order to ensure the system remains just. But over time, the way in which we have managed these distinct functions has caused unnecessary difficulties ranging from incompatible IT systems through to competing objectives and performance measures (DEn2)</p> <p>Information on most criminal cases originates with police involvement, but police IT is not well positioned to provide consistent data. The 43 forces have developed individual business processes supported by bespoke systems. As a result, there are some 2,000 force systems, connected through local infrastructure and managed locally by around 5,000 staff. (DEn3)</p> <p>What we did when we developed the OWI, knowing that we probably wanted to connect it to multiple police systems as well, we tried to make it as open and generic as we possibly can. We connected our system to around 10 different types of police systems and we did not have to make a modification at all in TWI. (LEn4)</p>	(In)compatibility of systems	Technical

	Technical	Synchronization of paper and digital information flow
		Suitability of criminal case data to become digital
Freedom to choose between paper and digital record keeping Challenge: • tool for both procedures must be present • Paper-Akt and digital act must punctual scanning permanently be synchronized Benefits: • decision-making body, the best determine appropriate way (D.A7)		
The experience is that 80% of the steps that needs to be taken to handle a large criminal file can be handled with electronically, however the remaining 20% is not possible. Examples are: you have to make a system which has the possibility for the electronic signature, which is not possible now. (LA1)		
There are no authorities sufficient confidence that electronic communications are secure. (D.D7)		
At this moment, we have a standard how these cases has to be presented to the prosecutor. It is not necessarily chronological. The standards say which things has to be first and last. The investigation in the middle is in the order that makes most sense. It is difficult to let a computing system make this decision. (LD4)		
Judicial professionals [prosecutors, judges] are very concerned about the safety of digitalisation of documents. (LD4)		
Legally we are still bound to the paper files. You have the possibility to send all paper documents as an electronic file to the court via E-file. But there has to be a paper document available according to law and therefore paper documents are used during court sessions. [...] We had already the possibility for using the digital signature for 12 years already. The people are using it from 2006 on now. Right now it is an everyday use. When a lawyer and a prosecutor want to communicate documents with each other, they can send over the documents digitally with the use of the digital signature. (LEs3)		
Right now the judges are printing the criminal case files, but in the future they are going to use digital versions of the criminal case files. These digital versions will be legally approved. Right now, the paper file is by law the original file. [...] They actually use paper files because this file is legally the original file. The paper file is still the file that should be brought to court instead of only the digital file. (LEs7)		
Currently the organizations cannot exchange multimedia files as videos and audio. We are working on that, we want to have the videos and voice recordings exchanged through the e-file. Currently we have the files in the system in court, but we do not have the multimedia files in the e-file system. The photos are available in the paper case. The paper case is still used besides the electronic case file. We are currently not fully digital yet. (LEs9)		
Data are not always transferable electronically even within partner organisations, resulting in further inefficiencies. (D.En3)		
There are no legal barriers to the use of or service of digital materials in the relevant statutes or in the Criminal Procedure Rules (the Rules) but see the section on the limitations on digital working above. (D.En11)		

There will be cases that you have to require things by paper, there are some cases that will never be suitable for complete digital information gathering, e.g. serious murder. That is about making sure if information is right and if information is proportionate, but you do not want to say that these cases need to be slimmed down in terms of evidence and evidence gathering. (I.En12)	Suitability of criminal case data to become digital	Technical
We recognized the electronic signatures. So all the witness statements police officers make can have digital signatures. We did not need any changes in the law, when we decided to start prosecuting electronically. (I.En4)		
It is not obligated to use ELC for all parties, but not for the police. It is hard to force them. The Ministry's would have to communicate that. (I.A5)	Organizational boundaries (of bureaucracy)	Managerial
It should be noted that a modernization of IT the support of the police and prosecutor's core tasks is a comprehensive task of great complexity. (D.D3)		
It is not just the structure of the criminal justice system that is complex. It also employs complex and bureaucratic processes. (D.En5)		
Most projects we have had, are small projects within the institutions, not cross-organizational. (I.D4)	(Lack of) experience and knowledge Resources	
The number of external consultants exceeded the expected level considerably and had the consequence that key tasks that should have been performed by the Police's own staff were also handled by external consultants. ... in some areas the Police failed to follow good practice for the management of government IT projects. (D.D2)		
The IT knowledge within the Police what not so far developed that they were able to design and implement POLSAG in such a way it was successful. (I.D6)		
We have many success stories by outsourcing the development the client systems, for example the court system. The prosecution system is made in-house. The small client systems that are connected to e-file are outsourced. (I.Es6)		
In support of this work, we need to make sure that all those responsible for preparing case files have the skills and support they need. To achieve this, we will ensure that police are trained and supported to prepare files - establishing whether existing guidance, training and awareness on preparation standards and proportionate and timely file build meet current requirements, and monitoring and improving quality and compliance with those requirements correctly. (D.En2)		
Key success factors are: - High level leadership - Management Sponsor for top level coordination - Legislation, Organization, Personnel, Budget - Setting direction and priorities - Active participation in the Steering Committee - Collection of requirements - Down handling of information (D.A1)	Leadership and project management	
Rigsrevisionen finds that the Ministry of Justice has been too reluctant to insist on implementing cross-sectoral solutions. (D.D1)		

There has not been sufficient management involvement and support to use datafolgesedIn. (D.D7)	Leadership and project management	Managerial
<p>The main barrier for the overall criminal justice chain to perform digital working is the lack of leadership. The experience with POLSAG was that there were no professional enough to be able to lead such a project. (LD5)</p> <p>I therefore find it also positive that the National Police since the start of Polsag has decided to change its management processes to include to strengthen the management and business involvement in police IT projects. ... I can inform you that the Ministry has launched a number of initiatives in order to strengthen the Ministry's supervision and overall management, including in relation to major IT projects of the ministry (DD3)</p>		
<p>It can be a bit difficult to get the parties have common goals, because that goals differ from their own goals. That is why we made the Forum for the directors to try to commit them for this common goal, and they can try to get it in the organization. But is still new, so we do not know if it is going to work. However, it looks like all the directors are interested in this. (LD4)</p>		
<p>There is a board (1) where all four authorities are represented plus the head of office where Holger is sitting plus Peter Greifenstein, and the Head of the IT department of each authority. Above, there is a board (2) with all the CEOs of the authorities. The first board has to report the board above them. That board decided to do this (this = ontwikkelingsdatafolgesedle). All four authorities must report to board. (LD2)</p>		
<p>Each agency had its own information system, each information system had its own architecture, business rules and own requirements for the submitting and exchange of data. None of the parties were ready to change this. We had quite a lot of debates, whereas the ministers decided that it just should be done, so we had no choice. We resolved it in a way that we had meetings with the users and working groups every week discussing and solving the problems that were there as a result of trying to implement each service into the system. (LEs10)</p>		
<p>The White Paper warns against procuring incompatible IT systems and taking decisions on the location of estates without considering the impact across the whole System. It also highlights measures to improve integration, including national leadership from the Criminal Justice Board and effective joint working by local partnerships. (D.En3)</p>		
<p>Arrangements for coordination of agencies are increasingly open to local variation across the country. In some places, local criminal justice boards still provide area-level coordination of local criminal justice partners. Boards brought together the chief officers of the local criminal justice partners to coordinate activity and share responsibility for delivering justice locally. (D.En3)</p>		
<p>Similarly this government is now pushing it to the same kind of ambition, within a context cross-government as a whole the importance of the moving towards digital ways of working is very much central. So it has always been something where governments have been talking about, but this government has made it an absolute core of their public sector reform, that moving towards digital models is key to delivering that. Within that, digitalisation of the criminal justice is the core bit. (LEn10)</p>		



Managerial	Leadership and project management	<p>At the local level the relationships between the police and the CPs are very good. Nationally, there is a degree of operating separately. Since 2012, the criminal justice partners came together in the efficiency and digital working programme. Therefore, the police and CPs have become closer in working together operationally. At the national level the agencies work together, but also at the local level there are implementation teams including the different criminal justice agencies. The success of joining the agencies together at different levels is built on working together instead of working on your own island. This is the first time, during the efficiency programme including working digitally, that agencies are working together in this way. At the moment, the relationships between the agencies are very strong, having a common vision and a common approach. (LEn1)</p>
	Concerns of (losing) autonomy	<p>Freedom to choose between paper and digital record keeping Challenge: • tool for both procedures must be present • Paper-Akt and digital act must punctual scanning permanently be synchronized Benefits: • decision-making body, the best determine appropriate way (DA7)</p>
	Resistance to change	<p>Justiz 3.0 is a project that started in the beginning of 2013 and in this projects plans are made on how to digitize and what should be digitized in 2020. There are judges and prosecutors involved in these meetings. Generally it shows that courts would like to stay using paper case files instead of working on electronic case files. (LA4)</p> <p>There is one major setback, resistance is historically by the judges the strongest. The public prosecutors, probably because they are a smaller group, probably because they are younger, they are more open minded towards automation. The body of judges is larger, they are more settled, therefore more reluctant to IT support. (LA5)</p>
	Regional differences	<p>There are many old judges that are used to work on the paper files. At the moment, the court information does not provide a comfortable way of using a digital file. (LEs7)</p> <p>Right now we have the situation that we have the digital court files, but we do not have good applications to work with digital court files. Because of that there are still paper files used in courts. And because courts are very conservative they do not want to use the digital case files. (LEs7)</p> <p>There are always regional different handlings of proceedings, so you have to find compromise between those perspectives. (LA6)</p> <p>This forum has concluded that the cooperation of authorities varies locally. This is caused by the fact that there are different needs and challenges locally, and therefore different local organisations. It is hard to get an overview of all these local areas about how the authorities cooperate. (LD5)</p> <p>Information on most criminal cases originates with police involvement, but police IT is not well positioned to provide consistent data. The 43 forces have developed individual business processes supported by bespoke systems. As a result, there are some 2,000 force systems, connected through local infrastructure and managed locally by around 5,000 staff. (D.En3)</p>

Managerial	Organizational differences Competing interests	
Political	Legislation and policies	<p>Also the prosecutors and the courts have their own computing department. The problem is to get these three to talk together in the same language. Difficult is to make the case systems connect to each other. (I.D4)</p> <p>The complexity of the system invites them; the large number of steps and the number of different agencies and people involved in even straightforward cases create multiple opportunities for a part of the process to go wrong. Often this means time wasted re-doing work or trying to find ways to work around obstacles like incompatible IT. It has resulted in a culture which has grown used to errors and re-work, and to a degree tolerates them, and a service that falls short of the standards the public rightly expects. (D.En2)</p> <p>The criminal justice system in England and Wales is complex, involving many different agencies, including police forces, the Crown Prosecution Service, the criminal courts, legal aid to fund legal defence, prisons, probation and youth offending teams. Too often, these organisations have worked in silos rather than working together: a fragmented system rather than a coherent service. This has been exacerbated by a target culture, which replaced professional discretion to do what was right. Agencies were encouraged to pursue individual targets: a focus on volumes rather than outcomes; quantity over quality (D.En5)</p> <p>The police are using independent systems, with their own standards. In addition, on the managerial level the attitude towards using new technologies and towards digitizing are different. The complexity between the sights differences, because one sight covers a more complicated area than others in terms of amount of crimes and amount of police forces. It is a combination of reasons: managerial drive; systems being different across the police; different levels of crimes. (I.En3)</p> <p>The authorities were - because of silo thinking - not motivated to implement datafolgesedIn. The authorities often have very different interests in the implementation of datafolgesedIn, as some authorities should pay the cost for performing changes in core systems, while other authorities "harvested" benefits. (D.D7)</p>
		<p>Legal aspects _ Electronic handling of files was provided in relevant laws before _ Only change: mandatory use of CDS in proceedings concerning unknown offenders (A.D2)</p>
		<p>The law allows the file to be electronically. Usually there are paper files and most documents are also digital available. There are separate systems/databases for police and justice. (I.A4)</p>
		<p>For the bigger picture of a digital file, probably legal changes do not have to be made, because in the law on criminal proceedings is a clause that everything can be done either on paper or digital. (I.A6)</p>
		<p>The bases for establishment and administration of databases, and supervision over the administration of databases is provided in Public Information Act. Act provides for: 1) the conditions of, procedure for and methods of access to public information and the bases for refusal to grant access; 2) restricted public information and the procedure for granting access thereto to the extent not regulated by other Acts; 21) the bases for establishment and administration of databases, and supervision over the administration of databases; 3) the procedure for the exercise of state supervision over the organization of access to information. (D.Es7)</p> <p>There were no laws that were blocking the design and development of the e-file system. The participants agreed that there was no need to change the law. (I.Es9)</p>

	Legislation and policies	Political
The core procedural acts changed before the establishment of the e-file. Also the statutes of the e-file were created by the government. We were able to develop the e-file system this soon because of the digital signature possibilities with the ID card and the x-road that provides the digital infrastructure. The idea to make all the data exchange in the public sector digital drove the criminal justice chain to become fully digital as well. (LEs11)		
Currently, the existing legislation limits both the types of proceedings in which video can be used, and the people who may participate in proceedings by video link. (D.En5)		
There is no requirement in relevant statutes or Rules for a signature to be in ink on paper (a so-called 'wet signature') or that a document must be signed in any particular way. A 'wet signature' is no more inherently reliable for confirming the authorship, integrity, or authenticity of a document than is a digital signature. (D.En11)		
The judiciary will be held in public. An important means to strengthen the public's trust in the judiciary is an effective public relations. The focus of the coverage away from criminal law and towards a holistic picture of the judiciary is to be routed. (D.A5)	Public scrutiny	
It should be transparent to the general public how long it takes to process a criminal case. (D.D1)		
In Estonia there is a law that if you have asked a person information once, you are not allowed to ask the person the same information again. For example, when I go to a register, systems can get information with the unique combination of the ID card and security code. Therefore, people do not have to fill out information all and all again. (LEs7)		
The system keeps logging all the activities that are done in the system. Consequently everyone can see if someone has been looking for your personal information by using the citizen portal. If someone has looked for your information you know who it was and then you can ask why. (LEs8)		
There was a need to get more statistical information of the performance of the chain to be able to show public how the system is performing and how the system works. (LEs11)		
The public will only have confidence in the system if they understand how it works, what they can expect, and how it is performing. Opening up public services will drive improvements in how those services are delivered and how their priorities are set. (D.En2)		
Budgetary Developments • Rising Requirements for IT • Low resources (personnel, Budget) • Cost / benefit Assessment (D.A7)	Budget	
The Ministry of Justice did not manage the funds appropriated to POLSAG in a satisfactory manner. The ministry did not include all costs in its appropriation request from 2007, but excluded costs that were essential for the implementation of the project and therefore – in the opinion of Rigsrevisionen – should have been included in the ministry's request. (D.D2)		

	Political	Budget
		Equality for prosecuting and defending party
		Judicial independence of courts
The budget is prepared by the minister of justice together with the managers and the director of the court. Then it is discussed in the council and approved by the minister. The budget of the court is part of the budget of the ministry. (lEs6)		
All CJS agencies have been working hard to increase efficiency; current budgetary constraints have provided a strong incentive to collaborate to meet this shared challenge. Agencies are working together to build on previous IT investment and break down the barriers to working independently of each other. (DEn1)		
What about the equality of the prosecutor to the defendant. They, by law, may not have advantages in comparison to the other party concerning presenting or defending the case. (lA3)		
All the parties of the proceeding are equal because they have the same information at the same time. • E-File is safer than the old system because the files are in the server demanding ID-card and passwords to enter. (DEs4)		
So when the Ministry makes a law, they have to follow it. However, the judicial decisions are completely independent, so there the Ministry cannot do anything. So the Ministry has some influence, but cannot give instructions as with the Prosecutors and the Police. (lD4)		
The court has the possibility to choose whether the paper file or the digital file is legally approved to use. (lEs7)		
The courts do not have to follow orders by the Ministry of Justice, they are independent. However, the Ministry of Justice decides on and provides the budget. The Rigsrevisionen argue that the Courts should be included in the organization and alignment of the criminal justice chain, even while they are in judicial terms independent. (lD3)		
The courts are of course independent from the Ministry of Justice. Besides, each court itself is independent, the president of a particular court is independent, and the judge is independent from the president of the court. The courts are at all levels independent. Still, the courts have some kind of mainstreaming, for example based on a performance management system. (lD6)		
But the court are independent and they use the budget independently to some extent. The budget of the IT is also included here. We have reserve budget as well, we finance it projects from this budget as you do not prepare for these investments. (lEs6)		
The ministry of justice has different tasks, but the court system is still independent. No one can interfere with the administration of justice. The ministry of justice has no right of command or disciplinary authority over judges. But they take part of the council for administration of courts. (lEs7)		
It is essential to retain the independence of operational policing and prosecutors, courts, defence and judiciary in order to ensure the system remains just. But over time, the way in which we have managed these distinct functions has caused unnecessary difficulties ranging from incompatible IT systems through to competing objectives and performance measures (DEn2)		

